## REMARKS

The present application was filed on April 5, 2001 with claims 1-20. In the outstanding Office Action, the Examiner: (i) provisionally rejected claims 1, 3-8, 10, 12-17, 19 and 20 under the judicially created doctrine of obviousness-type double patenting based on the copending U.S. patent application identified as Serial No. 09/638,320; (ii) rejected claims 1, 3-8, 10, 12, 14-17, 19 and 20 under 35 U.S.C. §102(b) as being anticipated by B. Schneier, "Applied Cryptography" (hereinafter "Schneier"); and (iii) rejected claims 2, 9, 11 and 18 under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Oorschot et al., "On Diffie-Hellman Key Agreement with Short Exponents" (hereinafter "Oorschot").

Regarding the §102(b) rejection of claims 1, 3-8, 10, 12, 14-17, 19 and 20 based on Schneier, Applicants traverse the rejection for at least the following reasons. It is well-established law that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Applicant asserts that the rejection based on Schneier does not meet this basic legal requirement, as will be explained below.

The present invention, for example, as recited in independent claim 1, comprises a method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret $g^{xy}$, where $g$ is the group generator known to both parties and $x$ is an index known to one party and $y$ is an index known to the other party, the group having a group operation and an inverse group operation. The method comprises the steps of one party generating a parameter $m$ by performing the group operation on $g^x$ and a function of at least the password, wherein any portion of a result associated with the function that is outside the group is randomized, and transmitting $m$ to the other party, whereby the other party may perform the inverse group operation on $m$ and the function of at least the password, and remove the randomization of any portion of the result associated with the function that is outside the group, to extract $g^x$ and calculate the shared secret $g^{xy}$. Independent claims 10 and 19 recite similar limitations in accordance with apparatus and article of manufacture aspects of the invention. Independent claims 8, 17 and 20 respectively recite similar limitations as claims 1, 10 and 19 from the perspective of the "other party."

Schneier does not teach or suggest each and every element of the claimed invention. For example, Schneier does not teach or suggest "any portion of a result associated with the function that

is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.

The Examiner appears to suggest (at page 5 of the Office Action) that Schneier discloses randomizing the part of a result lying outside the group, and subsequently removing that randomization. However, Schneier does not teach or suggest anything like that. In fact, Schneier assumes that the generator g used is "primitive" (see page 513 of Schneier), and thus generates every element in the multiplicative group mod n. Thus, everything is inside the group, and nothing is outside the group. Therefore, it is not possible for Schneier to disclose randomizing something outside the group. With regard to the randomness that Schneier mentions on page 520, this has nothing to do with the group. It is actually an extra key exchange, not involving any group operations, and is done only after the initial key exchange using Diffie-Hellman. Thus, it is quite clear that Schneier fails to teach or suggest "any portion of a result associated with the function that is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention.

For at least the above reasons, Applicant asserts that claims 1, 3-8, 10, 12, 14-17, 19 and 20 are patentable over Schneier.

Regarding the§103(a) rejection of claims 2, 9, 11 and18, Applicant asserts that such dependent claims are patentable over the combination of Schneier and Oorschot not only for the reasons above with respect to corresponding independent claims 1, 8, 10 and 17, but also because such dependent claims recite patentable subject matter in their own right.

Dependent claims 2, 9, 11 and 18 recite wherein the particular group, denoted as $G_{p,q}$, is a sub-group of a group $Z_p^*$ where $p$ and $q$ are prime numbers such that $p$ equals $rq + 1$ for a value $r$ co-prime to $q$, and wherein the step of randomizing any portion of a result associated with the function that is outside the group $G_{p,q}$ is performed by computing a parameter $h$, randomly selected from the group $Z_p^*$, raising the parameter $h$ to the exponent $q$ and multiplying $h^q$ by the result associated with the function. However, Oorschot fails to teach or suggest any such limitations.

Oorschot does indeed use the group $G_{p,q}$, but there is no mention (on pages 9 and 10, or anywhere else in the paper) about randomizing a value outside the group. In particular, in section 4 (pages 9 and 10), Oorschot mentions using safe primes with a generator of the whole multiplicative group mod p, so there is nothing outside the group to randomize. Oorschot also mentions an attack

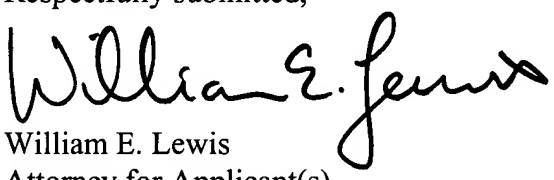
that raises the DH values to the q so that the result is in some small range. The point of this, though, is to make the result as non-random as possible, so that it can be guessed. Thus, Oorschot only discusses doing this when the co-factor is small. Subsequently, in section 5 (pages 10 and 11), Oorschot mentions restricting all operations to lie in a subgroup, but does not mention anything at all about operations outside the subgroup.

For at least the above reasons, Applicant asserts that claims 2, 9, 11 and 18 are patentable over the combination of Schneier and Oorschot.

Regarding the obviousness-type double patenting rejection of claims 1, 3-8, 10, 12-17, 19 and 20, Applicant traverses the rejection for at least the following reasons. As explained above, Schneier does not teach or suggest that "any portion of a result associated with the function that is outside the group is randomized . . . and remov[ing] the randomization of any portion of the result associated with the function that is outside the group," as recited in the claimed invention. Nonetheless, Applicant reserves the right to file a terminal disclaimer depending on the disposition of the present application.

In view of the above, Applicant believes that claims 1-20 are in condition for allowance, and respectfully requests withdrawal of the provisional double patenting, §102(b) and §103(a) rejections.

Respectfully submitted,



Date: July 13, 2004

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946